REMARKS

Claims 1-15 remain in this application for consideration. Claims 1, 5, and 13-15 have been amended.

Reconsideration of this application in light of the following remarks is requested.

I. Rejections Under 35 U.S.C. §112

Claims 3, 5, and 13-15 were rejected under 35 U.S.C. §112, second paragraph, for being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention.

Claim 1 has been amended to specify that the connection between the network processing system and the traversal client is a secure connection. Therefore, recitation of "the secure connection" in claim 3 now has proper antecedent basis. Accordingly, withdrawal of the rejection of claim 3 under 35 U.S.C. §112, second paragraph is requested.

Claims 5 and 13 have been amended to recite "the voice-over-Internet Protocol session" and thus now demonstrate proper antecedent basis for the claim language. Accordingly, withdrawal of the rejections of claims 5 and 13 under 35 U.S.C. §112, second paragraph, is requested.

Claims 13-15 have been amended to properly recite "the method" of the respective parent claims. Accordingly, withdrawal of the rejections of claim 13-15 under 35 U.S.C. §112, second paragraph, is requested.

II. Rejections Under 35 U.S.C. §102

Claim 1

Claim 1 recites the following:

> 1. A system for traversing a network address translation/firewall device, having a public side and a private side, with network traffic, the network traffic passing between a device on the private side and a device on the public side; the system comprising:
>
> a network processing system on the public side of the network address translation/firewall device, the network processing system operable to anchor network traffic to and from the private side of the network address translation/firewall device; and

> a traversal client on the private side of the network address translation/firewall device having a secure connection with the network processing system, wherein the traversal client is operable to pass packets through the network address translation/firewall device in order to create allocations in the network address translation/firewall device to allow the network traffic to pass between the private side device and the public side device, and wherein the traversal client does not reside in the path of the traffic between the private side device and the public side device.

Claim 1 was rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent Appl. No. 2003/0227903 to Watson ("Watson").

The PTO provides in MPEP § 2131 that

> *"[t]o anticipate a claim, the reference must teach every element of the claim...."*

Therefore, with respect to claim 1, to sustain this rejection the Watson reference must contain all of the above claimed elements of the claim. However, contrary to the Examiner's position that all elements are disclosed in the Watson reference, Watson does not disclose "a traversal client on the private side of the network address translation/firewall device having a secure connection with the network processing system, wherein the traversal client is operable to pass packets through the network address translation/firewall device in order to create allocations in the network address translation/firewall device to allow the network traffic to pass between the private side device and the public side device, and wherein the traversal client does not reside in the path of the traffic between the private side device and the public side device".

With regard to the claim 1 limitation of "a network processing system on the public side of the network address translation/firewall device, the network processing system operable to anchor network traffic to and from the private side of the network address translation/firewall device," the Examiner alleges such a system is disclosed by Watson at the following passage:

> According to one embodiment, firewalls are integrated with one or more of routers 130. For instance, the firewalls may be network address translation (NAT) firewalls that enable a private network with a multitude of private IP addresses to share one public IP address of router 130. A NAT protects networks 112 and 114 from unwanted Internet traffic from network 110. Particularly, the NAT firewall protects the networks by not letting any device outside of the network directly access any device (e.g., stations 150) on the network and behind the firewall.

> [0034] The NAT firewall acts as an interpreter between network 110 and/or networks 112 and 114. Network 110 is considered the `public` side and networks 112 and 114 are considered the `private` side. Whenever a device on the private side requests data from the public side (the Internet), the NAT device will open a portal between a private device and a destination device.
>
> [0035] In addition, the NAT firewall, or an associated proxy server, will translate the private address to a public address. This process is known as masquerading. When the public device returns results from the request, it is passed back through the NAT device to the requesting private device. Thus, a NAT enables a relatively large private network to use a small set of public IP addresses.

Watson, Paragraphs 0033-0035.

Here, Watson only discusses firewalls that may feature network address translation (NAT) functionality. The discussion of NAT firewalls in no manner describes or suggests a "a network processing system" on a "public side of the network address translation/firewall device" operable to "anchor network traffic to and from the private side of the network address translation/firewall device". For at least this reason, Watson fails to anticipate claim 1, and withdrawal of the rejection of claim 1 is thus requested.

With regard to the claim 1 limitation of "a traversal client on the private side of the network address translation/firewall device", the Examiner stated the following:

> Watson is directed to a system...comprising...a traversal client (PPG) on the private side of the network address translation/firewall device having a connection with the network processing system...

Office Action dated 2/16/2007, Page 3.

Applicant respectfully disagrees. For example, Figure 1 of Watson shows the following:

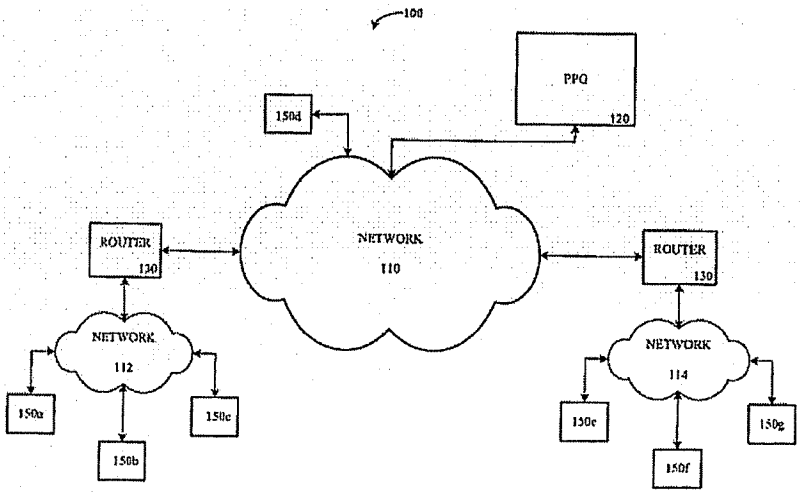

FIGURE 1

As clearly shown by Watson, the gatekeeper/public proxy (PPG) (120) is disposed on the public side of the NAT/firewall device. Moreover, Watson states the following regarding the PPG:

> FIG. 1 is a block diagram of one embodiment of a network 100. Network 100 includes networks 110, 112 and 114. In addition, network 100 includes **public proxy/gatekeeper (PPG)** 120...

Watson, Paragraph 0026 (in part, **Emphasis Added**).

Thus, PPG 120 is clearly depicted and described by Watson as a public device and is thus insufficient to disclose the traversal client "on the private side of the network address translation/firewall device" recited in the subject claim. For at least this reason, Watson is insufficient to anticipate claim 1, and such a notice is respectfully requested.

With further regard to the claim 1 limitation of "a traversal client on the private side of the network address translation/firewall device having a secure connection with the network processing system," Watson necessarily fails to disclose a private side transversal client having a secure connection" with the network processing system as Watson fails to disclose a traversal client "on the private side of the network address translation/firewall device" as discussed above.

Moreover, Watson is wholly silent with regard to secure connections. For at least these reasons, Watson is insufficient to anticipate claim 1, and such a notice is respectfully requested.

With further regard to the claim 1 limitation of "a traversal client on the private side of the network address translation/firewall device" that is "is operable to pass packets through the network address translation/firewall device in order to create allocations in the network address translation/firewall device," no private-side traversal client is described by Watson, and thus Watson is necessarily precluded from disclosing a traversal client "operable to pass packets through the network address translation/firewall device in order to create allocations in the network address translation/firewall device." For at least his reason, Watson is insufficient to anticipate claim 1, and withdrawal of the rejection of claim 1 is thus requested.

Therefore, the rejection is not supported by the Watson reference and should be withdrawn.

Independent claim 8 recites similar features as claim 1 and was rejected for the same rationale as claim 1. Therefore, the same distinctions between Watson and the claimed invention in claim 1 apply for claim 8. Consequently, it is respectfully requested that the rejection of claim 8 be withdrawn.

III. Conclusion

It is clear from all of the foregoing that independent claims 1-15 are in condition for allowance. Dependent claims 2-7, and 9-15 depend from and further limit independent claims 1 and 8 and therefore are allowable as well.

An early formal notice of allowance of claims 1-15 is requested.

Respectfully submitted,

Steven T. McDonald
Registration No. 45,999

Dated: May 29, 2007

HAYNES AND BOONE, LLP
901 Main Street, Suite 3100
Dallas, Texas 75202-3789
Telephone: 972/739-8644
Facsimile: 214/692-9075

I hereby certify that this correspondence is being filed with the United States Patent and Trademark Office via EFS-Web on the following date.

Date: May 29, 2007

Karen L. Underwood